Cultures & Conflits

58 | été 2005
Suspicion et exception

Biométrie et maîtrise des flux : vers une « géo-technopolis du *vivant-en-mobilité* » ?

Philippe Bonditti

Édition électronique
URL : http://journals.openedition.org/conflits/1825
DOI : 10.4000/conflits.1825
ISSN : 1777-5345

Éditeur :
CCLS - Centre d'études sur les conflits lilberté et sécurité, L'Harmattan

Édition imprimée
Date de publication : 1 juin 2005
Pagination : 131-154
ISBN : 2-7475-8911-0
ISSN : 1157-996X

Référence électronique
Philippe Bonditti, « Biométrie et maîtrise des flux : vers une « géo-technopolis du *vivant-en-mobilité* » ? », *Cultures & Conflits* [En ligne], 58 | été 2005, mis en ligne le 10 octobre 2005, consulté le 19 avril 2019. URL : http://journals.openedition.org/conflits/1825 ; DOI : 10.4000/conflits.1825

Biométrie et maîtrise des flux : vers une « géo-technopolis du *vivant-en-mobilité* » ?

Philippe Bonditti

1 Alors que sur fond de « guerre globale au terrorisme », les peuples d'Europe sont chacun à leur tour conviés à se prononcer sur leur éventuel devenir commun et ses possibles « formes », notre propos se centre sur le débat relatif au devenir de sa forme *territoriale et géographique*. Pour cela, nous nous proposons de poser la question de la relation transformée à l'*espace* et aux *territoires*, sous l'effet du recours accru à l'outil technique et plus spécifiquement à l'identifiant biométrique. A se fier à l'étrange crédulité de certains, les choses semblent être courues d'avance : « *nous sommes conscients que les technologies biométriques offrent de* nouvelles possibilités *pour mieux* combattre *l'utilisation de documents frauduleux à des fins criminelles ou* terroristes(...). *Nous sommes tous décidés à faire appel à la biométrie et tous convaincus qu'il y a urgence à le faire. Dès l'été* [2003]*, la lecture des passeports sera une lecture optique à Roissy et à Orly* » affirmait ainsi Nicolas Sarkozy, alors ministre français de l'Intérieur, lors de la présentation du groupe de travail franco-américain sur les techniques d'identification numériques en mai 2003. Pour pénétrer l'espace Schengen, mais aussi le *Homeland* américain et divers autres « espaces nationaux », il est exigé des individus qu'ils soient équipés de passeports *électroniques* comportant leurs données biométriques d'identification. Certes, ces décisions n'ont pas été sans débats. Leur mise en œuvre a suscité des résistances au sein du parlement européen (surtout), de divers parlements nationaux en Europe, de certaines commissions du Congrès américain aux Etats-Unis... Mais trop souvent, au sein de ces arènes, ce que l'on cherche à identifier c'est la meilleure technologie (empreintes digitales, iris, ADN...), trop souvent il n'y est question que d'efficacité, de coût, de temps de mise en œuvre, d'amortissement... autant d'éléments qui inféodent toujours la question du risque d'erreur aux arguments de la nécessité et toujours évacuent le politique.

2 Il est d'autres questions toutefois, soulevées par tant de voix, que nous souhaiterions reposer ici : la question de l'imaginaire politique à l'œuvre dans ces développements ;

celle des attentes nourries par ces croyances ignorantes en ces techniques ; celle des dynamiques sous-jacentes et préexistantes à ces développements contemporains ; celle, enfin, des effets de ces croyances sur nos sociétés. Et par-delà la « guerre au terrorisme » et les appels à un recours accru aux dites « nouvelles technologies », par-delà ce que certains perçoivent, non sans raison, comme une inquiétante généralisation de la surveillance, que d'autres encore disent nécessaire à la sécurité des populations, toutes ces questions nous semblent trouver un dénominateur commun : la relation contrariée au territoire – et à l'espace en général – qu'entretiennent les agences aux prérogatives dites de sécurité ; relation aujourd'hui informée par un vif imaginaire technicien et animée d'une forte angoisse, celle de la *mobilité*. Questionner ainsi le devenir des territoires, notamment géographiques, sous l'effet du recours accru à l'outil numérique, en nous centrant primordialement sur la relation entretenue tant aux territoires qu'à la technique, permet, nous pensons, de faire surgir, d'abord, les logiques à l'oeuvre dans le contrôle et la surveillance des individus ; ensuite leur convergence de part et d'autre de l'Atlantique ; enfin une lecture *autre* de cette liberté de mouvement si vivement débattue, de manière si contradictoire parfois.

3 Nous inspirant des réflexions de Lucien Sfez sur l'imaginaire qui joue en fond de ce recours aux nouvelles technologies[1] et à l'avènement d'une *technopolis*, nous insisterons ici sur cette inversion de la relation entre politique et technique que pointe l'auteur de *Technique et idéologie* ; la technique devenant « servante-maîtresse » du politique vient soumettre ce dernier aux impératifs de la nécessité, « *substituant à la fiction de la technique, le sérieux de sa prétendue objectivité* »[2]. Les croyances que cette technique cristallise et les discours de la nécessité dans lesquelles ces dernières s'incarnent alors et en premier lieu, se posent en obstacle au traitement politique de questions pourtant fondamentalement politiques posées par des phénomènes globaux comme les pratiques transnationales de violence et les flux migratoires. Mais c'est peut-être davantage encore à la suite des travaux de Michel Foucault que viennent s'inscrire ces quelques pages.

4 Les développements relatifs à l'introduction de l'identifiant numérique à des fins de contrôle des individus s'inscrivent en effet pleinement dans la prolongation des analyses du processus de « gouvernementalisation » de l'Etat décrit par l'auteur de *Surveiller et punir* ; processus entamé au XV^{ème} siècle et par lequel « *l'*Etat de justice *du Moyen-Age, devenu au XVème et XVIème siècle l'*Etat Administratif, *s'est trouvé petit à petit 'gouvernementalisé'* »[3], s'émancipant partiellement des contraintes du territoire, pour s'incarner dans un Etat de population/gouvernement. L'Etat n'est « *plus* [alors] *essentiellement défini par sa* territorialité, *par la surface occupée, mais par une masse : la masse de la population avec son volume, sa densité, avec bien sûr, le territoire sur lequel elle est étendue, mais qui n'en est en quelque sorte qu'une composante* »[4]. Michel Foucault suggérait ainsi un double glissement : celui d'un « Etat de territorialité » vers un « Etat de population » et celui d'un « pacte de territorialité » vers un « pacte de sécurité » entre le souverain et le peuple. Dans le premier cas, le Prince assure en premier lieu la sûreté et l'unité d'un espace territorial, contre des intrusions extérieures, et par le renforcement de la frontière, définissant ainsi progressivement l'espace territorial d'exercice illimité du pouvoir souverain[5]. Dans le second cas, la « sécurité » n'est pas tant celle du territoire que de la population en elle-même conduite au travers de technologies biopolitiques.

5 Les développements à l'œuvre en matière de numérisation des documents d'identification, la manière dont est aujourd'hui envisagée le recours à l'outil technique biométrique, les formes de croyances qu'il cristallise, brillent ainsi bien davantage par

l'approfondissement de logiques anciennes que par quelconque nouveauté. Il nous semble ainsi tous prolonger et approfondir les logiques historiques de contrôle et de surveillance mise en évidence par Michel Foucault dans ses cours au collège de France à la fin des années 1970. Et c'est en quelque sorte l'inclinaison que connaît ce processus sous l'effet du recours accru à l'outil numérique que nous nous proposons ici de discuter. Pour cela, nous tenterons de situer notre analyse au croisement, d'une part, de ce processus animé d'une dynamique historique, et actualisé dans l'Etat de population et, d'autre part, du processus plus récent de numérisation des documents d'identification des individus. En portant ainsi une attention particulière à cette rencontre entre les formes de croyance en la technique et les conditions spatio-temporelles depuis lesquelles elles se forgent et s'expriment, nous espérons éclairer une tension, un affrontement entre un imaginaire spatio-temporel technicien – et sa rationalité réticulaire sous-jacente – d'une part, et l'imaginaire spatial de la souveraineté – avant tout territorial et fragmenté. En cela, nous ne prétendons pas questionner l'outil technologique dans ses spécificités techniques, mais bien la relation, informée par des imaginaires spatio-temporels non nécessairement compatibles, qu'entretiennent professionnels de la politique et de la sécurité à l'outil technique.

6 Inscrivant alors nos conclusions à la croisée[6] des analyses de Gilles Deleuze, Michel Foucault et Paul Virilio, nous tenterons d'émettre quelques propositions pour l'analyse des effets de ce recours accru à l'outil numérique sur la frontière et la trajectoire historique de construction de l'Etat. Nous serons alors amenés à constater combien, ce qui se joue en fond de ces développements renvoie bien davantage à l'articulation entre, d'une part, un souci de gestion/maîtrise du vivant-en-mobilité et, d'autre part, les cadres spatio-temporels de la souveraineté depuis lesquels sont développés ces mécanismes de gestion. Comment la gestion des flux, du mouvement, de la mobilité (et l'imaginaire qui la sous-tend) est-elle pensée, énoncée, formulée et surtout organisée depuis les cadres de pensée de la souveraineté et son imaginaire spatio-temporel propre ? Nous tenterons alors d'éclairer la manière dont le recours aux pratiques de numérisation et, plus généralement, le rapport entretenu à l'outil technique, informatique (et aux espaces qu'il génère), s'appuie sur la prétention souveraine pour en retracer ses lignes d'activation tout en reconduisant le principe de fonctionnement fondamental du *politique* en système déjà constitué d'intérieurs et d'extérieurs[7]. En d'autres termes, ce que nous tentons de montrer, c'est la redéfinition des correspondances entre des trajectoires temporelles, des mouvements, des flux, d'une part, et des séparations spatiales, des démarcations, d'autre part.

Langage, technique et spatialisation de la menace

7 Les développements centrés autour de l'introduction de l'outil numérique dans les pratiques d'authentification des papiers et d'identification des individus prennent corps dans un tissu épais de textes, d'énoncés, de discours, de rapports qui décrivent, qualifient et spatialisent la « menace terroriste ». Et si, de part et d'autre de l'Atlantique, ces strates discursives diffèrent par certains aspects, la voie militaire de la lutte contre le terrorisme trouvant notamment un plus large écho aux Etats-Unis, ces différences ne portent toutefois pas selon nous sur les logiques historiques de transformations des appareillages d'Etat détenteurs de prérogatives dites de sécurité, aux Etats-Unis comme en Europe. Et c'est bien, de notre point vue, dans la manière dont la menace se voit progressivement

articulée à la technique, depuis une dizaine d'années aux Etats-Unis et plus récemment en Europe, qu'émerge de lourdes convergences d'approche.

8 Depuis la fin des années 1960, il s'est en effet opéré, aux Etats-Unis, un glissement progressif dans l'énonciation de la menace terroriste. L'analyse de l'ensemble discursif mobilisé à sa description révèle ainsi différents procédés de spatialisation. Cette strate de textes sur la menace, écrits et/ou parlés, nous informe ainsi des caractéristiques et des formes de celle-ci. Mais, « *informer c'est* [aussi] *faire circuler un mot d'ordre* » rappelait Gilles Deleuze. « *On nous communique de l'information, on nous dit ce que nous sommes censés être en état ou en devoir ou être tenu de croire. L'information est le système de contrôle* »[8]. Informer sur la menace c'est l'offrir, dans des formes bien spécifiques, à ces croyances en la technique que nous évoquions. Informés par l'imaginaire spatio-temporel de la souveraineté depuis lequel ils sont énoncés, tous ces discours, dans leur prétention à dire le vrai tout autant que le souhaitable, tous ces textes de lois, dans leur prétention normative à définir le légal et l'illégal, en produisant, pour les premiers, ou en admettant, pour les seconds, des vérités sur les formes de cette menace, viennent actualiser cette dernière dans l'ordre discursif et textuel, lui conférant certaines caractéristiques, notamment spatiales. Ce faisant, ils dessinent les formes, les limites, juridiques, légales, réglementaires, morale mais aussi spatiale du « nous-collectif »[9].

9 L'analyse de cet ensemble textuel et discursif révèle, aux Etats-Unis, trois mouvements dans la description de la menace terroriste. Trois mouvements qui cohabitent depuis la fin des années 1970 et la mise sur l'agenda politico-militaire américain de la lutte anti-terroriste. Le premier articule la menace (mais aussi les formes de la réponse devant lui être opposée[10]) sur les coordonnées spatiales traditionnelles la territorialisant, l'associant à des aires géographiques bien précises et/ou des Etats souverains[11]... Le second tend à l'inverse à l'arracher du territoire, à la déterritorialiser pour insister sur sa structure réticulaire et la re-localiser dans un ordre social, qui s'étend au-delà des espaces nationaux géographiques. Il décrit alors des individus regroupés en cellules terroristes, inscrites en réseaux, distribuées à la surface de la planète, et dotées d'une certaine autonomie par rapport à un organe de commandement. Le troisième mouvement à l'œuvre dans cette strate discursive de qualification de la menace terroriste est venu offrir un nouveau support à cette rationalité réticulaire, l'associant, à partir du milieu des années 1990, à la technique, définissant alors des menaces d'un nouveau type, dont les cibles, les infrastructures critiques et autres systèmes informatiques ne sont plus nécessairement matériels, mais dont la destruction engendrerait les plus graves dommages pour la nation.

10 Les deux premiers mouvements de territorialisation et de dé-territorialisation coexistent dans les analyses américaines sur le terrorisme depuis vingt-cinq ans. Nous ne reviendrons pas ici sur les origines de cette tendance qui suppose une véritable généalogie des discours et des acteurs qui les prononcent. Mais la « guerre au terrorisme » dans laquelle est engagée l'Amérique de Georges Bush, les rhétoriques de l'Axe du mal, ou bien encore les nouvelles mesures de contrôle aux entrées et sorties du territoire national, ne peuvent être comprises que si l'on considère ce double processus de territorialisation-déterritorialisation et ses enjeux : pour engager la force militaire dans la lutte contre le « terrorisme », un Etat doit être désigné, désigné comme menaçant ; désigné comme le sont depuis 1979 les « Etats dits sponsors du terrorisme » encore appelés *Rogue States* ; désigné comme l'a été l'Afghanistan dans les jours ayant suivi les attaques sur New York et Washington[12]. Inversement, une analyse en termes de

réseaux, qui déterritorialise la menace implique un engagement plus marqué du renseignement dans toutes ses dimensions et ne va pas sans le risque d'une mise sous surveillance généralisée des individus.

11 Si l'Europe et ses Etats membres ont toujours été peu enclins à rendre publique, officialiser et institutionnaliser une liste « d'Etats sponsors du terrorisme », personne ne nie toutefois l'existence d'une telle liste, très largement discutée, circulant de manière informelle entre services nationaux, et structurant, au moins partiellement, les politiques nationales de lutte anti-terroriste[13]. L'Europe publie en revanche sa liste des organisations dites « terroristes », participant à son tour à ce mouvement décrivant la menace en réseaux[14]. Plus récemment, les arguments ayant prévalus à la signature de l'accord PNR entre l'Union européenne et les Etats-Unis, mais aussi à l'intégration des identifiants biométriques dans les passeports, visas et autres cartes nationales d'identités, viennent accentuer cette convergence transatlantique orchestrée par la prise en considération de l'élément technique[15].

Technique et spatialisation de la menace

12 Le troisième mouvement discursif, associant donc menace et technique, est à la fois plus ample et plus lourd de conséquences. Il ne vient plus seulement articuler la menace sur le squelette des frontières territoriales, mais sur celui, bien technique, des systèmes informatiques qui présentent cette double caractéristique d'être à la fois encrés dans l'ordre territorial (des serveurs, des disques durs, des rooters, des détecteurs, des capteurs, des stations d'acquisition, des scanners, des caméras... accumulés dans des bâtiments, dispersés en divers point de la surface de la planète) et générateur d'espaces non euclidiens d'échanges et de communication (cyberespace), faits de lignes entendues ici comme jonction[16].

13 La menace vient alors s'actualiser dans le discours sous deux formes principales : celle d'attaques portées contre des infrastructures critiques – présentées aux Etats-Unis comme support de la nation/patrie (*Homeland*) –, et celle d'attaques électroniques, portées au moyens de puissants programmes informatiques (virus...) contre les systèmes eux-mêmes[17]. La menace terroriste ne se résume plus seulement à des « Etats sponsors du terrorisme », non plus seulement à des réseaux de « cellules terroristes » dispersées à travers la planète. Les analyses, américaines notamment, sont alors marquées par l'ontologie du « *worst case scenario* », évoquant une menace bactériologique ou un Pearl Harbour électronique. Elles décrivent dans une naïveté candide, des individus « terroristes », certes inscrits en réseaux, mais désormais aux moyens de... ces banals outils de notre quotidien que sont ordinateurs portables et autres téléphones cellulaires. Très tôt, le FBI développe une activité de veille et d'alerte, produisant rapports et autres « *Cybernotes* », prenant ainsi une part active au développement d'une nouvelle catégorie de crime : le cybercrime. L'organe militaire américain, qui développe ses stratégies cybernétiques depuis la fin des années 1960 et les premières heures de l'ARPA, dispose de son champ lexical propre, centré sur les *Information* (IW)et *Cybernetic* (CYW) *Warfares*[18]. Développées en complément de stratégies plus anciennes (*Transnational Infrastructure Warfare* (TIW), *Asymmetric Warfare*, *Asynchronous Warfare*), elles tombent toutes sous la dénomination générique de *Networkcentric Warfare*[19].

14 Le 11 septembre 2001 n'est venu inscrire aucune rupture majeure dans ce rapprochement progressif opéré entre menace et technique, renvoyant toujours aussi classiquement à un

souci historique de spatialisation de la menace (et, par un même mouvement, du « soi-collectif »). Mais, ces multiples lectures et interprétations, informées ces dernières années par un vif imaginaire technicien, ont tout de même eu cet effet majeur d'activer à égale intensité des deux premiers mouvements de territorialisation/dé-territorialisation, celui associant menace et technique. Aux Etats-Unis, la Maison Blanche a progressivement élevé la sécurité du cyberespace et des systèmes informatiques au rang de problème de sécurité nationale. D'abord en nommant Richard Clarke conseiller pour la sécurité du cyberespace. Ensuite, en réorganisant profondément l'architecture bureaucratique de l'anti-terrorisme. Enfin, en publiant la *Stratégie nationale de sécurité du cyberespace*[20]. Ce document situe la sécurité du cyberespace en rapport à celle de la Patrie (*Homeland*) et à la sécurité nationale, distinguant au passage les unes des autres et établissant entre elle, nous y reviendrons, une étrange hiérarchie : de la sécurité du cyberespace et de sa fiabilité, dépendraient le bon fonctionnement de l'économie nationale, des infrastructures dites critiques et des organes de défense nationale. Fruit d'une « rationalisation extensive » des activités relatives au nouveau souci de sanctuarisation du territoire national aux Etats-Unis, ce document vient en premier lieu réintégrer au *Homeland*, le cyberespace et les systèmes informatiques. Le territoire n'est plus ici seulement considéré dans sa dimension géographique ; il est aussi câbles et faisceaux d'ondes transportant des données numériques et supportés par des infrastructures nationales dites critiques. Cette stratégie – d'ailleurs dite *nationale* et *de sécurité* – légitime ainsi l'intervention de l'Etat, le réinvestit dans sa figure de souverain face à un espace discontinu, à délimiter, à légiférer et, à en croire certains hauts responsables militaires américains, à pacifier. Eventuellement territorialisable, mais alors en des points dispersés et débordant largement le cadre territorial géographique, cet espace ainsi pris en considération dans les discours et autres rapports, conduit à une redéfinition de la notion de frontière, dans sa forme plus que dans sa fonction comme nous le verrons.

15 Si la logique militaire et sa dimension stratégique ne gouvernent pas aujourd'hui une Europe, qui heureusement n'a pas les moyens d'une telle ambition, certains développements récents rappellent encore une fois la convergence de certaines logiques, celles notamment ayant prévalues à l'établissement de la Division du cybercrime au sein du FBI en 2002. Une nouvelle fois, l'analyse peut alors dépasser le cas des Etats-Unis, suivre ce dénominateur commun que sont la technique et les croyances auxquelles elle donne lieu, pour se porter vers l'Europe. La sécurité du cyberespace, bien que non encore nécessairement posée comme première, y devient progressivement une préoccupation de premier plan. En France, la mise en place en mai 2000 de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC, ministère de l'Intérieur) marque le développement des activités de police en vue de la répression de deux types d'infractions pénales : celles « *directement liées aux technologies de l'information et de la communication (TIC) dans lesquelles l'informatique est l'objet même du délit* [et celle] *dont la commission est liée ou facilitée par les TIC et pour lesquelles l'informatique n'est qu'un moyen* »[21]. L'établissement, plus récemment encore (mars 2005), du Centre pour les Technologies de Sécurité Intérieure (CTSI) au titre de la « *modernisation des instruments de lutte contre le terrorisme* »[22],témoigne aussi de cette préoccupation. Placé sous la tutelle administrative du ministère de l'Intérieur, il n'en est pas moins développé sur la base de la Délégation Générale de l'Armement[23] du ministère de la Défense (révélant au passage un autre mouvement de convergence, celui-ci entre police, armée et renseignement). Mais c'est peut-être avec le récent rapport « Chantier sur la lutte contre la cybercriminalité » qu'apparaît avec plus de force encore la convergence des logiques de

part et d'autre de l'Atlantique. Révélant à son tour l'étrange relation entretenue au cyberespace et à la technique, ce rapport vient légitimer l'intervention de l'Etat français face à ce qui est présenté comme un « *nouvel espace.* [Un] *espace 'informationnel'* [qui] *vient désormais s'ajouter aux espaces terrestre, maritime et aérien, dont la protection et la sécurité entrent naturellement dans le champ des compétences régaliennes de l'Etat*»[24]. En cela, il s'offre bien en résonance de la Stratégie nationale de sécurité du cyberespace des Etats-Unis, même si là encore, l'approche se révèle moins stratégique et militaire, bien davantage posée en termes de cybercrime et de police.

Une relation ambivalente à l'outil technique

16 L'analyse croisée des discours et des textes associant plus spécifiquement « menace terroriste », sécurité nationale, sécurité des réseaux informatiques et du « cyberespace », révèle un rapport ambigu à ce dernier. Bien que présenté, nous venons de le voir, comme partie intégrante de l'*espace national,* pleinement intégré au *Homeland* aux Etats-Unis, en voie d'intégration à l'espace Schengen en Europe[25], il est aussi posé comme *source de danger et de menaces*, se faisant alors l'allié du « terrorisme » dans ses projets les plus meurtriers. Cyberattaques contre des systèmes informatiques en voie d'intégration viennent dès lors cohabiter, dans le discours, avec des attaques plus classiques, portées contre des infrastructures dites critiques, structure/support technique d'un « cyberspace » dématérialisé et déterritorialisé.

17 On fait enfin appel à lui comme à l'*outil salvateur*, recourant à ses bases de données, et tandis que Nicolas Sarkozy fait état des nouvelles possibilités offertes par les dites « nouvelles technologies », John Negroponte, nouveau Directeur du renseignement aux Etats-Unis insiste sur « *des capacités non encore révélées* »[26]. Sondé en permanence, à la recherche de communications suspectes, le cyberespace devient l'outil électronique de renseignement par excellence, tout à la fois source d'information et lieu d'accumulation et de stockage d'un savoir digital d'Etat sur les individus, compilé dans des bases de données, en voie de constitution et d'intégration partielle. Aux Etats-Unis, la *National Security Agency*, mandatée pour scruter, examiner, scanner en permanence cet espace, coordonne le réseau mondial de surveillance électronique Echelon[27]. L'ARPA (l'agence de développement de programmes hautement technologiques du Pentagone) développe pour sa part le *Terrorism Information Awareness Program* appelé à :

> « (...) révolutionner la capacité des Etats-Unis à détecter, classifier et identifier les terroristes étrangers – et décoder leurs plans – et par là permettre aux Etats-Unis de mener des action appropriées pour prévenir et faire échouer les actions terroristes. (...) Techniquement, le programme TIA se concentre sur le développement : 1) des architectures pour une base de données anti-terroriste de grande ampleur, pour des éléments des systèmes qui soient associés à la population des bases de données, et pour intégrer des algorithmes et des outils analytiques d'initiatives mixtes ; 2) de nouvelles méthodes de peuplement des bases de données à partir des sources existantes, créer de nouvelles sources innovantes et inventer de nouveaux algorithmes pour extraire, combiner et affiner l'information pour une inclusion ultérieure dans la base de données ; et, 3) de nouveaux modèles, algorithmes, méthodes, outils, et techniques révolutionnaires pour analyser et corréler l'information dans la base de données pour en tirer des renseignements ajustables en temps réel »[28].

18 Du Système d'Information Schengen (SIS I et II) aux programmes de contrôle des entrées et sorties du territoire américain CAPS II et US VISIT ; des bases de données d'Europol au

nouveau Visa Information System (appelé à être branché sur le SIS II), le cyberspace est ici considéré dans sa dimension non territoriale certes, mais surtout pour le dispositif de contrôle et de surveillance qu'il constitue. Par le recueil et surtout l'accumulation des données (traces) digitales qu'il autorise, ces pratiques visent non seulement l'identification des individus, mais leur *localisation* dans l'ordre territorial géographique, et la reconstitution de leurs trajectoires, ceci au moyen du recueil et du recoupement des traces numériques, certaines biométriques. Et tout ce qui peut ainsi être collecté doit être enregistré, conservé, accumulé dans ces bases de données. Mais en recourant ainsi de manière active aux bases de données, entièrement constitutives de ce « cyberespace », les agences de sécurité participent activement de sa construction. L'interconnexion croissante de ces bases est entièrement guidée aux Etats-Unis par le souci de partage de l'information (*Information Sharing*) entre agences de sécurité (militaires, polices, renseignement, douanes) mais aussi entre secteurs privé et public. Une logique dans laquelle l'Europe n'est pas, là encore, totalement exempte. Les fournisseurs d'accès Internet sont désormais vivement incités voire, dans certains cas nationaux (comme en France), légalement tenus de conserver les données des connections des Internautes ; certaines lois organisant même l'accès à ces bases à des autorités compétentes[29]. Et pour cette raison supplémentaire que ces bases de données recèlent les identités supposées des individus, nécessaires à la sécurisation des territoires et des populations, elles doivent non seulement être protégées – et cela au même titre que le territoire géographique –, mais deviennent aussi la condition de sécurité du territoire.

19 Dans leur prise en considération de l'élément technique et du cyberespace, les analyses dites de sécurité se trouvent comme prisonnières des modes traditionnels de sécurisation. Elles viennent s'offrir en relais des logiques historiques de protection de l'espace territorial, ne faisant que les projeter sur un nouvel espace à sécuriser : à la sanctuarisation du territoire comme condition de sécurité des populations, vient s'ajouter la sanctuarisation du cyberespace et de ses bases de données comme condition de sécurité du territoire géographique et, en conséquence, des populations – ceci par une étrange forme de raisonnement tautologique conduisant à assurer la sécurité par la sécurité.

20 La technique biométrique vient établir ce lien crucial entre, d'une part, le contrôle des individus en un point d'un espace territorial donné et repérable dans les coordonnées euclidiennes de la plus simple des géométries et, d'autre part, ces systèmes de bases de données en voie d'intégration détenant les éléments nécessaires à l'identification des individus. Il se dessine un dispositif de contrôle et de surveillance, incarné dans ces systèmes informatiques intégrés et s'activant à plusieurs niveaux, à la fois sur et par-delà les espaces territoriaux/nationaux.

La traçabilité comme mode de gouvernement des hommes ?

> « Le projet [de carte nationale d'identité biométrique] vise la mise en œuvre d'un document hautement technologique qui *prouvera le droit d'un individu à se trouver sur le territoire national*. Ce projet de carte d'identité est un *projet global*, pensé pour couvrir chaque individu autorisé à être ici (...). Ce document montrera que tout le monde appartient à notre société qu'il soit né ou ait choisi de s'établir ici, ou de rester le temps d'un travail ou de ses études »[30].
>
> « Le programme INES – identité nationale électronique sécurisée – est un *projet global* qui consistera à : Fusionner, simplifier et sécuriser les procédures de

> demande de passeport et de carte nationale d'identité (CNI) ; Améliorer la gestion de ces titres dans de nouvelles applications ; Délivrer des titres hautement sécurisés conformes aux exigences internationales ; Offrir aux citoyens les moyens de *prouver leur identité* sur Internet et de signer électroniquement, afin de favoriser le développement de l'administration électronique »[31].

21 Tirés du *White Paper* du *Home Office* britannique, et du Programme INES du ministère français de l'Intérieur pour justifier de la nécessité de mettre en place une carte nationale d'identité biométrique, ces extraits illustrent clairement l'esprit dans lequel prend aujourd'hui corps ce mouvement ample et diffus de numérisation des documents d'identification. Les projets français et britanniques sont des initiatives récentes sous-tendues par la logique historique d'accumulation d'un savoir total sur les individus sur un espace territorial donné. Elle renvoie à l'exercice d'une technologie positive de pouvoir. Elle renvoie à ce *rêve politique de la peste* évoqué par Michel Foucault et au traitement des pestiférés à partir du XVIII[ème] siècle en France. Mise en quarantaine, la ville en état de peste est d'abord l'objet d'un recensement rigoureux par lequel chaque habitant se voit inscrit dans les registres de la ville établis à cet effet. Elle est ensuite rigoureusement divisée en quartiers et districts, prise dans un quadrillage serré, chaque rue se voyant assigner un surveillant, chaque quartier, un inspecteur, chaque district, un responsable de district. Chacun était tenu de rester chez soi. Et chaque jour, les surveillants devaient circuler dans les rues, frapper aux portes ; les occupants devant chacun à leur tour se présenter à la fenêtre. Et celui qui ne se présentait pas était alors déclaré malade et par conséquent, dangereux. Et tout ce qui était ainsi observé devait être qualifié, rapporté et enregistré dans les registres de la ville.

> « Une mobilité croissante combinée à des technologies poussées rend de plus en plus difficile la protection et l'authentification de l'identité des individus. La sécurité et la prospérité des citoyens britanniques s'en trouvent menacée par les migrations illégales, le crime organisé et le terrorisme. C'est la raison pour laquelle la technique des passeports biométriques est d'ores et déjà mise en œuvre ailleurs en Europe et aux Etats-Unis »[32].

22 La logique à l'œuvre derrière ces propositions britannique et française cohabite, à l'échelle européenne, avec une autre logique, celle-là de démarcation, de rejet : celle du visa Schengen. Cette dernière ne renvoie plus au traitement des pestiférés, mais à celui des lépreux.

23 Durant tout le Moyen-Age et jusqu'au tournant du XVIII[ème] siècle, le traitement des lépreux impliquait « *une pratique sociale qui comportait d'abord un partage rigoureux, une mise à distance, une règle de non contact entre individus ou groupes d'individus* »[33]. La « mise en quarantaine » de la population des lépreux « *en dehors des murs de la ville, au-delà des limites de la communauté* », était le pendant d'un souci de « purification » salvateur de la population. Ainsi étaient constituées deux masses d'individus, étrangère l'une de l'autre. Ainsi était instituée une frontière entre une population, que l'on voulait maintenir saine, et une population considérée comme malade. C'était, explique Michel Foucault, une pratique de rejet, d'exclusion, de marginalisation. Cette logique de l'exclusion sous-tend, aujourd'hui encore, toute politique de visa, et donc aussi celle du visa Schengen. Une politique de mise à distance des étrangers, de maintien des migrants indésirables en dehors des frontières de l'espace Schengen. Elle se double, comme l'ont montré Didier Bigo et Elspeth Guild[34], d'un souci de contrôle à distance, d'un contrôle qui ne s'effectue plus à la frontière, à l'entrée du territoire considéré, mais dans le pays de départ des individus et qui rappelle (de manière inquiétante dans leur complémentarité comme dans

leur correspondance) les logiques développées pour la protection du *Homeland* américain. Cette logique réhabilite, symboliquement, la frontière entre un espace intérieur dont il faut s'assurer la maîtrise, et un espace extérieur, cet espace confus du lépreux, du migrant indésirable et indésiré.

24 Antithétiques en tout point, ces deux technologies de pouvoirs n'en cohabitent pas moins dans les sociétés occidentales depuis le tournant du XVIII^{ème} siècle. Elles sont, pour l'auteur de *Surveiller et punir*, les deux grandes logiques de contrôle des individus que l'Occident ait connu. Leur combinaison, prise dans le mouvement de numérisation, dessine un dispositif global de contrôle des individus dont l'analyse révèle deux niveaux. Le premier (national) implique une analyse fine et détaillée de ce qui vit et bouge sur un territoire donné et se fait au moyen de la carte nationale d'identité biométrique. Le second s'attache au contrôle des entrées et sorties d'un espace territorial donnée, englobant le premier et pris dans un processus serré de sécurisation. Il porte la focale sur les flux, les mobilités et trouve pour instrument le visa Schengen.

Biométrie et re-spatialisation du « faire vivre et laisser mourir » : vers une « géo-technopolis du *vivant-en-mobilité* » ?

25 Deux niveaux différenciés de contrôle des individus donc, mais une tendance commune : leurs recours à l'outil numérique. S'il apparaît légitime de penser que l'outil biométrique ne débouchera pas sur les effets escomptés (fin des fraudes, arrestation des « terroristes » et autres migrants déclarés illégaux), le recours au contrôle biométrique n'est toutefois pas dépourvu d'effets. Au-delà de l'illusion de la nouveauté, il approfondit en fait les logiques historiques de contrôle en les systématisant et en les automatisant[35]. Il transforme aussi la frontière et incline la trajectoire historique de l'Etat dans ses activités de contrôle et de surveillance.

26 La réhabilitation de la frontière dans sa fonction de démarcation depuis le 11 septembre cohabite avec la technicisation du contrôle et des documents d'identification. Observable à travers la mise en place du *Homeland Security Department* aux Etats-Unis et les velléités proches en Europe, elle redessine une carte des territoires à sécuriser pour mieux protéger les populations des dangers de l'extérieur. Elle fige les espaces là où les recours à la biométrie révèlent à l'inverse l'angoisse de la mobilité, du mouvement et de la permanence des flux. La frontière se trouve prise, dès lors, dans une dynamique de redéfinition qui ne porte pas tant sur sa fonction que sur sa forme. Sous l'effet de la technique, elle est prise dans un mouvement de pixellisation/pointillisation, glissant de la ligne au point. Elle passe d'une forme linéaire et continue à un ensemble discontinu de points, de points de contrôle à l'embarquement qui sont autant de points de connexion à ces bases de données (registres digitalisés) dans lesquelles sont progressivement enregistrées les identités supposées des individus contrôlés.

27 La numérisation des documents d'identification et de la frontière radicalise en outre la logique de contrôle à distance du visa Schengen. D'abord pensée pour être appliquée aux migrants non ressortissants des Etats-membres, avant de s'appliquer aux ressortissants des pays de l'Union, elle rend possible la simultanéité du contrôle et de la sanction. Le contrôle du migrant non désiré – auquel l'entrée dans l'espace Schengen a déjà été refusée, et qui se trouve donc déjà être enregistré dans les bases de données – correspond à un refus immédiat d'embarquement. Contrôle à distance, sanction immédiate. Couplée à la logique du *profiling*, cette numérisation crée ses propres zones de stigmatisation et de

marginalisation, rendant possible des traitements différenciés. Dans le cas du migrant non désiré s'applique ce droit du faire vivre et laisser mourir, dont Michel Foucault a bien montré qu'il est progressivement venu se substituer au droit de souveraineté, formulé suivant le choix souverain du faire mourir *ou* laisser vivre[36]. Faire vivre une population, corps biologique multiple en mobilité de l'espace Schengen, et détenir pour une durée indéterminée[37] ou laisser mourir ceux auxquels l'entrée est refusée ? Dans le cas de l'individu dont le profil répondrait à celui, préétabli, d'un « terroriste » par exemple, la numérisation du contrôle ouvre la possibilité d'une surveillance plus poussée, d'une traçabilité accrue, chaque contrôle générant sa trace numérique, dont le recueil et la conservation autorisent, désormais, éventuellement, la reconstitution des *trajectoires*.

28 Avec les propositions britannique et française de carte nationale d'identité biométrique se dessine la dispersion de ces points de contrôle à l'intérieur même du territoire. Ils viendront s'ajouter à ceux déjà existants du maillage technique serré qui innerve nos sociétés (borne de retrait d'argent, connections à l'Internet, carte magnétique d'accès aux transports en commun...). Le projet d'équiper, à terme, les forces mobiles de police britanniques de systèmes de lecture adaptés aux documents biométriques d'identification, vient s'ajouter aux obligations données aux fournisseurs d'accès Internet de conserver les données de connections des internautes, et nourrir un peu plus encore ce « rêve politique de la peste » décrit par Michel Foucault.

29 Gilles Deleuze écrivait que « *si modèle* [foucaldien] *il y a, c'est le modèle de la 'peste', qui quadrille la cité malade et s'étend jusqu'au moindre détail* ». La numérisation nous paraît comme venir réaliser la synthèse des deux grands types de contrôle éclairés par Michel Foucault en décalant leur objet qui, après le territoire et le corps, s'exerce désormais aussi sur la mobilité, par les corps (qui ne sont plus seulement *objets* mais *instruments* des technologies de pouvoir), et par-delà les territoires.

30 Il s'opère toutefois un renversement majeur qui montre que si modèle il y a, ce n'est peut être pas aussi précisément celui de la peste. Ce renversement s'opère au niveau de la mobilité : dans le modèle paradigmatique de Foucault, ce sont les contrôles qui sont inscrits dans une certaine mobilité à travers la circulation des surveillants, là où, dans ce qui est à l'œuvre, dans ce mouvement de numérisation de la frontière et des outils d'identification, les contrôles sont essentiellement (même si non exclusivement) réalisés en des points fixes et figent les mobilités. Dans le modèle de Foucault, tout est figé et le pouvoir s'exerce à plein lorsqu'il circule sans résistance entre ces éléments figés, lorsque contrôle et surveillance sont comme indifférenciés dans un espace mis en quarantaine. Mais dans les développements contemporains, tout est mobile, changeant, fuyant, et l'une des conditions de l'efficacité de l'exercice du pouvoir semble résider dans la complémentarité qui se dessine entre surveillance et contrôle, entre ancrage territorial des points de contrôle et parfaite circulation des informations entre eux. Les logiques développées viennent poser le contrôle comme la condition d'une « surveillance efficace ». Le contrôle individualise et, s'appliquant en un point géographique précis, permet la localisation. Le contrôle, c'est le moment où tout s'arrête dans l'attente de la réponse, c'est le moment plus ou moins long, parfaitement localisable, générant de multiples connexions, et auquel tout individu est soumis plusieurs fois par jour : contrôle lors des mouvements ou consultations bancaires, lors des paiements au moyen d'une carte à puce, ou d'identifiant de connexion si les requêtes sont émises depuis Internet ; contrôle lors de l'accès aux métros ou à certains bâtiments au moyen de cartes magnétiques ; contrôle lors de la visite médicale (carte vitale)... Autant de contrôles qui

pour l'heure s'appuient sur des éléments d'identification différenciés mais en voie d'unification. Le corps multiple de la population, pris dans sa dualité individu-masse, se trouve ainsi être l'objet de ces procédures de contrôle en de multiples points de ses échelles. L'intégration des identifiants biométriques dans les documents d'identités vient alors révéler la prise en considération, non plus seulement de ce corps multiple de la population dans ses caractéristiques biologiques, mais dans ses multiples mobilités, dans sa dynamique et sa fluidité. Si Michel Foucault ne distingue pas clairement surveillance et contrôle dans son modèle paradigmatique de la peste, c'est peut-être parce que dans la modélisation qu'il propose, surveillance et contrôle sont co-constitutifs là où, dans ce qui se joue aujourd'hui, contrôle et surveillance s'inscrivent dans une inquiétante complémentarité. L'acte de contrôle émerge toujours dans un ensemble placé sous surveillance constante, continuellement soumis à des mécanismes de visibilisation, faisant de la surveillance, dans le modèle de Michel Foucault comme dans les développements bien contemporains, une condition d'un contrôle efficace par des agents autorisés (on pensera ici au cas paradigmatique des systèmes de vidéosurveillance, fonctionnant comme système d'alerte[38]). Mais l'acte de contrôle vient aussi organiser les conditions d'une surveillance efficace. Le contrôle doit permettre d'activer des mécanismes plus poussés de surveillance s'appuyant sur la *traçabilité* du sujet considéré.

31 Parce que tout cela prend forme dans un système de plus en plus imprégné par des pratiques d'identification en voie de numérisation, il devient possible de retracer la trajectoire des individus. Dans cet ensemble en mobilité à plusieurs échelles (locale, nationale, globale ; urbaine, régionale, planétaire), le processus de numérisation et les adaptations des pratiques de contrôle et de surveillance d'Etat qu'il génère redessinent les lieux et les modes d'exercice de l'autorité souveraine, en opérant une démultiplication de la capillarité du pouvoir. Il en découle un recentrage de l'appareil d'Etat spécifiquement affecté au contrôle et à la surveillance autour du souci de conduite de la « masse-en-mobilité », et fait émerger des outils, l'ordinateur, l'identifiant biométrique, la base de données, la station d'acquisition, le logiciel de traitement de données... et surtout la *trace numérique* ainsi qu'une technique bien spécifique : la *traçabilité.* La part active de l'appareil d'Etat dans ce mouvement fait qu'il se développe au prix d'un paradoxe fondamental : la démultiplication de la capillarité du pouvoir, la réticulation extrême de ses modes d'exercice rendue possible par l'interconnexion progressive des bases de données, entament les fondements tant géopolitiques que juridiques de l'Etat. Le mode/type souverain d'exercice du pouvoir se répand alors dans sa forme réticulée et déterritorialisée, au-delà de la frontière, aux moyens d'architectures techniques de *gestion de la mobilité à divers échelles* (i.e. bases de données interconnectées dans des systèmes informatiques intégrés) assurant une certaine distribution du *vivant-en-mobilité* dans l'espace. Il en découle une redéfinition des lieux d'application du pouvoir souverain[39] et des adaptations dans l'ordre géopolitique. La frontière se trouve dès lors prise dans ce mouvement de pointillisation/pixellisation qui correspond à la distribution de ces points de contrôle à la surface de la planète, contrôle mis au service d'une politique de protection à distance du *Homeland* d'une part, et de l'espace Schengen d'autre part.

32 Tous ces développements, qu'il s'agisse de l'interconnexion des bases de données des appareillage bureaucratiques ordonnés au renseignement et à la lutte contre le terrorisme – aux Etats-Unis comme en Europe[40] –, du recours aux identifiants biométriques et de l'accumulation d'information sur les individus par le recueil des traces numériques qu'ils génèrent quotidiennement, renvoient tous et pour partie à la notion

d'espace, au souci de spatialisation (de ce « Eux » distinct du « Nous ») et à la distribution du corps multiple de la population dans des espaces discontinus. Le territoire, et plus largement l'espace ont toujours joués comme contrainte dans le processus historique de gouvernementalisation de l'Etat de justice du Moyen-Age : le moment souverain vise la délimitation de cet espace national territorial ; le moment disciplinaire assure bien une certaine distribution des individus dans divers espaces clos (école, armée, usines, hôpitaux...), au sein de l'étendue territoriale, elle-même délimitée par la frontière ; avec le moment biopolitique se dessine aussi la distribution et la protection du corps de la population, là encore prise sur un espace donné. Mais, rappelle Deleuze, « *Foucault pensait que nous entrions dans un type de société nouveau. Bien sûr il y a toutes sortes de restes des sociétés disciplinaires, pour des années et des années, mais nous savons déjà que nous sommes dans des sociétés d'un autre type qu'il faudrait appeler, selon le mot de Burroughs* (...) *des sociétés de contrôle* »[41]. Et ce sont bien les adaptations à cette sortie des sociétés disciplinaires, et notamment ces adaptations ayant une composante spatiale, qu'il nous a ici été donné de discuter.

33 Ce qui est en train de s'opérer, c'est la recherche d'une correspondance *via* les identifiants biométriques entre, d'une part, les squelettes techniques des réseaux de bases de données contenant les informations relatives aux individus et autour desquels les administrations se réorganisent et, d'autre part, le squelette bien géographique des frontières. Et tandis que la frontière glisse de la ligne au point, le mouvement historique de transformation de l'Etat et de l'art même de gouverner connaissent une nouvelle inclinaison. Le recours à la technique qui autorise le relevé systématique et automatique des traces digitales et leur accumulation dans des réseaux en voie d'intégration sont la marque de la stratégie de l'état d'urgence en voie de constitution. Paul Virilio, dans ses travaux sur la vitesse en politique[42], a déjà posé le cadre d'appréhension de cette nouvelle inclinaison de l'Etat. En le paraphrasant, nous pourrions écrire : « *nous voilà au coeur de l'espace contemporain, espace 'stéréopolitique' où les catégories du temps et de l'espace sont traitées en simultanéité par l'Etat, l'état terminal d'information* (...) *Recueillir de plus en plus rapidement, puis capitaliser l'information sur la matière et sur les corps (territoriaux, sociaux, animaux...), voilà la stratégie de l'état d'urgence* (...) *en voie de constitution* (...) ; *harmoniser au mieux des intérêts d'un centre abstrait, les réseaux relationnels, voilà la forme moderne du pouvoir totalitaire* »[43].

34 Paul Virilio nous offre ainsi de solides outils pour l'analyse de cette relation transformée au territoire sous l'effet du recours accru à la technique. Virilio fouille ce lien entre territoire et technique (notamment militaire). La logique qu'il décrit est effectivement celle qui sous-tend la doctrine de *transformation* des armées américaines. Mais la disparition de la distance territoriale que Virilio pointe en « accident » de l'accroissement de vitesse généré par la technologie, cet anéantissement des distances territoriales trouve son pendant dans le maintien rigide et meurtrier de certaines distances et les logiques de police à distance et de projection des forces, ici prise au sens littéral. Mais c'est bien parce que Paul Virilio a su si justement décrire le développement des technologies de l'armement dans leur affranchissement progressif de la distance et de la contrainte territoriale, qu'il est possible de percevoir cet autre versant du gain de vitesse, celui de la fixation des distances, à la suite, notamment, de Didier Bigo et Elspeth Guild. Fixer des distances, pour mieux maintenir les indésirables au-delà des limites de l'espace considéré, ceci par un contrôle à distance, lui-même rendu possible par l'accroissement de vitesse de circulation des informations entre des agents inscrits en réseaux et mandatés pour faire que s'exécute à distance l'autorité souveraine[44].

35 Toutes ces évolutions, qui s'accélèrent chaque jour un peu plus, au gré de la lutte antiterroriste, fournissent des pistes à ceux dont le travail consiste à questionner l'Etat dans ses prérogatives de contrôle des individus. Décaler le regard à la recherche des agences, services, bureaux et individus qui s'activent derrière la figure de l'Etat et qui disent parler en son nom ne suffit plus. Il faut désormais, pour qui s'intéresse aux pratiques de surveillance, identifier les bases de données, leurs interconnections et toujours, ceux qui les gèrent ; et tenter de conduire cette « *étude socio-technique des mécanismes de contrôle* [et de surveillance]*, saisis à leur aurore,* (...) *catégorielle* [pour] *décrire ce qui est en train de s'installer à la place des milieux d'enfermement disciplinaires, dont tout le monde annonce la crise* »[45].

NOTES

1. Sfez L., *Technique et idéologie*, Paris, Seuil, 2002.

2. Sfez L., *ibid.*, p. 15.

3. Foucault M., *Sécurité, Territoire, Population. Cours au Collège de France, 1977-1978*, Paris, Seuil/ Gallimard, 2004, p. 112.

4. Foucault M., *op. cit.*, p. 113.

5. Nous renvoyons ici à Foucault M., *Naissance de la Biopolitique. Cours au Collège de France, 1978-1979*, Paris, Gallimard/Seuil, 2004, pp. 14-15.

6. A la croisée... ou peut-être dans la continuité de cette correspondance entre Foucault et Virilio rappelée par Deleuze.

7. Voir à ce propos Walker R.B.J., « After the Future: Enclosures, Connections, Politics », in Falk R., Ruiz L.E.J., Walker R.B.J., *Reframing the International. Law, Culture, Politics*, New-York/Londres, Routledge, pp. 3-25 : « *Nous nous trouvons être comme pris dans une série de puzzles, à la fois logiques et pratiques, tâchant d'identifier un extérieur à une conception du politique qui se trouve déjà être constituée en système d'internes et d'externes* » (p. 6). Voir aussi du même auteur, Walker R.B.J, *Inside/Ouside*, Cambridge, Cambridge University Press, 1993.

8. Deleuze G., *Deux régimes de fous*, Paris, Les Editions de Minuit, 2003, p. 299.

9. Walker R.B.J, *Inside/Ouside*, *op. cit.*, voir notamment le chapitre 6 : « The Territorial State and the Theme of Gulliver », pp. 125-140.

10. A ce propos, voir Bonditti P., « Digitalizing Surveillance. Networking antiterrorism », article préparé dans le cadre du programme cadre de recherche Challenge (6ème PCRD). Ce texte sera prochainement consultable sur Internet : http://www.libertysecurity.org/.

11. Cette tendance est plus particulièrement observable dans le rapport annuel du département d'Etat, *Patterns of Global Terrorism.* On la retrouve aussi dans les doctrines militaires (notamment doctrine des conflits de basse intensité) et les diverses stratégies nationales de sécurité (notamment la doctrine Lake). A ce propos voir Klare M.T., *Low-intensity Warfare*, New York, Pantheon Books, 1988 ; et *Rogue States and Nuclear Outlaws*, New York, Hillang Wang, 1995.

12. On notera au passage que l'Afghanistan n'est jamais apparu dans la liste des Etats-sponsors du terrorisme.

13. Entretiens avec un haut responsable de l'Unité de coordination et de lutte anti-terroriste (UCLAT) du ministère français de l'Intérieur (avril 2001, février 2005).

14. L'établissement d'une telle liste ne va pas, en Europe, sans de vifs affrontements politiques, entre les Etats membres rappelant combien les procédures de qualification et de désignation de ces organisations ne peuvent être comprises sans un détour par les impératifs de politiques nationales.

15. Voir dans ce même numéro l'article de Mitzilegas V., « Contrôle des étrangers, des passagers, des citoyens : surveillance et antiterrorisme ».

16. C'est William Gibson dans le roman de sciences fictions *Neuromancien*, qui le premier fait usage du terme *cyberspace* pour définir : « *Une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts mathématiques... Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain. Une complexité impensable. Des traits de lumière disposés dans le non-espace de l'esprit, des amas et des constellations de données. Comme les lumières de villes, dans le lointain* », in Gibson W., *Neuromancer*, New York, Ace Books, 1984 pour la version originale. Je me réfère à la traduction française, *Neuromancien*, Paris, La Découverte, 1988 p. 64. Pour une analyse de l'imaginaire à l'œuvre derrière les représentations du cyberespace, voir l'excellente contribution de Musso P., « Le cyberespace, figure de l'utopie technologique réticulaire », *Sociologie et société*, vol. 32, n°2, pp. 31-56 (texte disponible dans son intégralité sur http://www.erudit.org/).

17. Aux Etats-Unis, on se référera aux conclusions du groupe de réflexion inter-agences sur la politique anti-terroriste américaine créé par la directive présidentielle n°39, en 1995. Il y est évoqué l'existence de menaces exercées contre des infrastructures américaines: « *On décida qu'au vu de l'envergure des infrastructures critiques et de la multiplicité des sources et des formes d'attaque, le Cabinet Committee devrait considérer non seulement les menaces terroristes aux infrastructures mais aussi les menaces émanant d'autres sources. Le Comité doit aborder tant les attaques 'physiques' traditionnelles (par exemple les bombes) que les 'cyber' attaques, électroniques, aux infrastructures (par exemple une attaque d'un ordinateur ou d'un système de communication)* », (notre traduction). Voir *Memorandum on Critical Infrastructure Security*, Office of the Attorney General, Washington DC 20530, 14 mars, 1996.

18. Voir à ce propos « Global Threats and Challenges: The Decades Ahead », *Prepared Statement before the Senate Armed Services Committee*, Lieutenant General Hughes P. M., U.S. Army, Director, Defense Intelligence Agency, *Washington D.C.*, 2 février 1999.

19. « *Le 11 septembre a démontré de manière sans doute plus intense que n'importe quel autre évènement l'étendue du changement du monde ces dernières années. Nous sommes loin de l'époque à laquelle les guerres mettaient des mois à être lancées et des années à être menées. Les ennemis des Etats-Unis ne se déplacent pas au rythme d'armées ou de navires dans un champ de bataille mais au rythme de l'information se déplaçant dans le cyberespace, les téléphones cellulaires et les satellites – rendant cette nouvelle ère sans doute l'ère la plus dangereuse à laquelle les Etats-Unis aient jamais eu à faire face* », (nous traduisons), Office of the Assistant Secretary for Public Affairs (Pentagone), *Facing the Future: Meeting the Threats and Challenges of the 21st Century. Highlights of the Priorities, Initiatives, and Accomplishments of the U.S. Department of Defense2001-2004*, février 2005, p. 33.

20. « Le cyberespace est essentiel à la *homeland security* et à la *national security* ; sa sécurité et sa fiabilité soutiennent l'économie, les infrastructures critiques et la défense nationale (...) Ce document (...) est une stratégie des pas que feront les Etats-Unis pour sécuriser les réseaux et systèmes des technologies de l'information qui sont nécessaires à la défense de l'économie nationale et au bon fonctionnement des services essentiels. Ces réseaux, et les équipements et logiciels des technologies de l'information qui les font fonctionner ensemble composent notre cyberespace », (nous traduisons / citation italique), *The National Security Strategy to Secure Cyberspace*, version préliminaire, septembre 2002, p. 1 et 17.

21. http://www.premier-ministre.gouv.fr/chantiers/garantir_securite_tous_152/lutter_insecurite_50077.html

22. *Ibid.*

23. « Le renseignement policier se met aux techniques de pointe », *Le Figaro*, 14 janvier 2005, et http://www.premier-ministre.gouv.fr/chantiers/garantir_securite_tous_152/lutter_insecurite_50077.html

24. *Chantier sur la lutte contre la cybercriminalité*, Rapport présenté par Thierry Breton, Remis à Monsieur le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales le 25 février 2005, p. 1.

25. *Chantier sur la lutte contre la cybercriminalité*, Rapport présenté par Thierry Breton, *op. cit.*, p. 17.

26. Voir Negroponte J., *Hearing Before the Senate Committee on Intelligence*, 12 avril 2005.

27. Voir à ce propos : Campbell D., *Interception Capabilities 2000. Development of Surveillance Technology and Risk of abuse of Economic Information,* STOA, Parlement européen, PE 168 184, avril 1999.

28. On se référera ici à : Total Information Awareness System Description Document (TIA/SDD), Version 1.1, Information Awareness Office, July 19, 2002. Disponible sur : http://epic.org/privacy/profiling/tia/tiasystemdescription.pdf Initialement appelé *Total* Information Awareness (TIA), ce programme, informé des plus vifs fantasmes du contrôle technologique total, ne visait pas moins, à terme, que la mise en registre de l'ensemble de la population mondiale dans ses coordonnées biométriques et la mise en réseau de tout un maillage de systèmes de surveillance et d'identification à distance. En juillet 2003, le Congrès américain a décidé de ne pas reconduire le financement de ce programme. Mais les imaginaires du contrôle fonctionnent à plein régime...

29. Aux Etats-Unis, on se référera aux Patriot Act I et II ainsi qu'au cadre légal développé pour l'utilisation du programme Carnivore par le FBI (programme pensé pour la surveillance des personnes suspectées de crime. Il fonctionne tel un « système renifleur » (*sniffer*) et permet au FBI de récupérer auprès des fournisseurs d'accès Internet (FAI) les paquets de données échangées entre l'utilisateur (surveillé) et le FAI. Voir les travaux du *Electronic Privacy Information Center* (EPIC) : http://epic.org/privacy/carnivore/foia_documents.html. Voir aussi les travaux du *Center for Democraty and Technology* (http://www.cdt.org/). On pourra notamment consulter les auditions de Charles X. Dempsey devant les diverses commissions du Congrès. Voir aussi: Cole D., Dempsey J. X., *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*, The New Press, 2002.

30. Home Office, *Identity Cards: The Next Step,* novembre 2003, p. 7 (nous traduisons et nous soulignons).

31. Le programme INES (Identité nationale sécurisée), Secrétariat général, Direction de programme INES, ministère de l'Intérieur, de la Sécurité intérieure et des Libertés locales, 31 janvier 2005, p. 1.

32. Home Office, *Identity Cards: The Next Step*, novembre 2003, p. 7 (nous traduisons).

33. Nous nous inspirons ici très directement des écrits de Michel Foucault dans *Surveiller et Punir*, Paris, Gallimard, chapitre 3, « Le panoptisme », pp. 229-264 ; *Les Anormaux*, Paris, Seuil/Gallimard, pp. 40-46 ; *Il faut défendre la société*, Paris, Seuil/Gallimard, pp. 213-235.

34. Bigo D., Guild E., La mise à l'écart des étrangers : La logique du Visa Schengen, *Cultures & Conflits*, Paris, L'Harmattan, n°49, printemps 2003.

35. Lyon D., *Surveillance after September 11*, Cambridge, Polity, 2003, 197 p. et notamment le chapitre 3 : Automating Surveillance, pp. 62-88.

36. Foucault M., *Il faut défendre la société*, *op. cit.*, p. 214.

37. Voir à ce propos Valluy J. (dir.), L'Europe des camps, *Cultures & Conflits*, Paris, L'Harmattan, n° 55, printemps 2005.

38. A ce propos on se réfèrera à la mise en place, en octobre 1998, dans le quartier de *Newham* à Londres, d'un maillage de 140 caméras de vidéosurveillance, branché sur le célèbre logiciel de reconnaissance faciale *Mandrake*. Ce logiciel de traitement de données vise le recoupement en

temps réel des images ainsi saisies avec la centaine de photographies de délinquants précédemment enregistrées dans les bases de données de deux commissariats du quartier. Les autorités de *Newham* affirment que le système d'alerte ainsi formé doit permettre de prévenir les opérateurs des caméras dès qu'une correspondance est établie entre les photographies numériques des délinquants d'une part, et les images saisies d'autre part... La technologie ici développée recourt au traitement algorithmique de données. A ce propos, voir les travaux précédemment cités de Stephen Graham et David Wood.

39. En cela, notre réflexion est probablement inspirée du questionnement de Jef Huysmans (« Discussing Sovereignty and Transnational Politics », in Walker N., *Sovereigny in Transition.* Oxford, Hart, 2003, pp. 209-227), qui pose la question de savoir « dans quelle mesure les re-imaginations de la location et de la nature des sciences politiques diluent-elles ou re-articulent-elles la matrice de la souveraineté ? » (« *to what extend re-imaginations of the location and nature of the politics dilute or re-articulate the matrix of sovereignty* ») (p. 209).

40. On se réfèrera ici pour l'Europe aux travaux de Thomas Mathiessen et notamment *On Globalization of Control: Towards an integrated Surveillance System in Europe*, *Statewatch*, Londres, 2000.

41. Deleuze G., « Qu'est ce que l'acte de création », in *Deux régimes de fous. Textes et entretiens 1975-1995*, édition préparée par David Poujade, Paris, Les Editions de Minuits, 2003, pp. 299.

42. Virilio P., *Vitesse et politique*, Paris, Gallilée, 1977 ; voir aussi Der Derian J., *The Virilio Reader*, Malden (E-U)/Oxford (RU), Blackwell Publisher, 1998.

43. Virilio P., « L'Etat d'urgence et l'autogestion de l'espace », disponible sur : http://www.increvablesanarchistes.org/articles/1968_81/urbanisme_autogestion.htm

44. Sur la correspondance des travaux de Michel Foucault et Paul Virilio, voir Deleuze G., *Foucault* , Paris, Les Editions de Minuits, 1986 (2004 pour l'édition considérée), pp. 49-50.

45. . Deleuze G., « Post-scriptum sur les sociétés de contrôle », *Pourparlers*, Paris, Les Editions de Minuits, (1990 pour la première édition), 2003 pour la présente, p. 246.

RÉSUMÉS

Nous nous proposons ici d'explorer les imaginaires politiques à l'œuvre derrière le recours accru à l'identifiant biométrique et plus généralement aux nouvelles technologies. Ceci pour rappeler, d'abord, combien le recours à l'outil biométrique, informé par des imaginaires spatio-temporels non nécessairement compatibles, s'inscrit pourtant pleinement dans la prolongation des logiques historiques de contrôle et de surveillance des individus par l'Etat ; pour insister ensuite sur la convergence, de part et d'autre de l'Atlantique, des logiques à l'oeuvre dans la transformation des pratiques de contrôle et de surveillance des individus par l'Etat, convergence ici principalement relayée par l'imaginaire technicien et sa spatio-temporalité propre ; pour tenter de montrer enfin que ces développements renvoient en fait bien davantage à l'articulation problématique entre, d'une part, un souci de gestion/maîtrise du *vivant-en-mobilité* et, d'autre part, les cadres spatio-temporels de la souveraineté depuis lesquels sont développés ces mécanismes de gestion.

The aim of this paper is to explore the imaginary at play in the resort to biometry. First, to show how this resort, informed by spatio-temporal imaginaries that are not necessarily compatible, are to be totally inscribed in the scope of the historical logics underlying people control and

surveillance ; second, to insist on the convergence, on both sides of the Atlantic ocean, of these logics at play in the transformation of state control and surveillance practices, convergence that is reinforced/intensified by the technical imaginary and its spatio-temporality ; finally, to try to show that all those developments relate to the tricky articulation between the concern to manage « life in mobility » on the one hand, and the spatio-temporal framework of the sovereignty within which the mechanism aiming at controlling « life in mobility » are developed on the other.

INDEX

Mots-clés : Exception, suspicion, ELISE, biométrie, mobilité, flux

AUTEUR

PHILIPPE BONDITTI

Philippe BONDITTI est doctorant à l'IEP de Paris. Chargé de recherches au Centre d'Etudes sur les Conflits et membre de l'équipe française des programmes européens ELISE et CHALLENGE.